ABSTRACT

In a communication system (1), a header comprising information, preferably being related with a device-type associated commitment, is additionally provided with a signature for that information. The signature guarantees the authenticity of the header information. The signature is tamper-resistantly created in a first device (20), preferably based on at least tamper-resistant device-type specific information of the first device (20). The header information and the signature are communicated to a content provider (10), where the signature is verified before accepting the device-type associated commitment to be valid. Such signatures can preferably be used in systems using HTTP or SMTP.

(Fig. 3)